From: Moody, Dustin (Fed)
To: D., pqc-forum
Subject: Re: [pqc-forum] Parameter selection for the selected algorithms
Date: Friday, December 02, 2022 02:02:04 PM ET

Hi Dan,

What we meant was: There are various possible improvements in cryptanalysis, including: (i) optimization of lattice algorithms to improve the locality of memory access, (ii) building memory hardware that reduces the cost of non-local memory access, and (iii) other (more fundamental) improvements in the attacks. It seems unlikely that (i) and (ii) alone will be sufficient to cause Kyber-512 to fall below category 1 security, in realistic models of security that take these costs into account.

Dustin

From: pqc-forum@list.nist.gov on behalf of D. J. Bernstein
Sent: Friday, December 2, 2022 10:38 AM
To: pqc-forum
Subject: Re: [pqc-forum] Parameter selection for the selected algorithms

Derek Atkins writes:
> I don't think any clarification is required. I think it is quite
> obvious that NIST is claiming A, B, and C, and is not claiming D, just
> as you "guess"ed.

Hmmm. Taking the original words "small enough" literally wouldn't match what A says; and readers who aren't sticking to literal interpretations could easily understand the "barring ... unlikely" part to indicate D. I think A+B+C-not-D is a reasonable interpretation, but I'm not at all sure that this is what NIST meant. NIST should clarify.

---D. J. Bernstein

To view this discussion on the web visit https://groups.google.com/a/list.nist.gov/d/msgid/pqc-forum/20221202153847.69158.qmail%40cr.yp.to.